AMENDMENTS TO THE CLAIMS

Claim 1-2. (canceled)

Claim 3. (currently amended) The ~~method~~ system of claim [[1]]29 wherein the client's request~~ed form of~~ to access ~~to~~ the certain user-specific information in the data store identifies a desired subject matter to be accessed and a method of accessing the desired subject matter and wherein comparing the ~~determined~~ set of default access preferences with the intended use by the client ~~with the default access control instruction~~ further comprises[[;]] determining if the set of default access preferences ~~control instruction~~ permits the client to access the desired subject matter; and determining if the set of default access preferences ~~control instruction~~ permits the identified method of accessing the desired subject matter.

Claim 4. (canceled)

Claim 5. (currently amended) The ~~method~~ system of claim [[4]]32 wherein creating the access control rule comprises updating ~~the~~ a list of access permissions ~~control list~~ such that ~~the~~ said list of access permissions ~~control list~~ reflects whether the user accepted or rejected the at least one option.

Claim 6. (currently amended) The ~~method~~ system of claim [[1]]29 ~~further comprising:~~ wherein the client determining if the client has a local copy of the ~~requested~~ certain user-specific information in the data store before transmitting the ~~access~~ request ~~message~~[[;]], the client retrieving said local copy of the ~~requested~~ certain user-specific information if the local copy is available[[;]], the client determining if said local copy of the ~~requested~~ certain user-specific information is current[[;]], and transmitting the ~~access~~ request ~~message~~ only if said local copy of the ~~requested~~ certain user-specific information is not available and not current.

Claim 7-8. (canceled)

Claim 9. (currently amended) The ~~method~~ system of claim [[1]]29 ~~further comprising:~~ wherein the access control engine determining if the client has an access subscription right to the ~~requested~~ certain user-specific information in the data store[[;]] and the access control engine permitting the client to have access to the ~~requested~~ certain user-specific information in the data store if the client has the access subscription right to the ~~requested~~ certain user-specific information in the data store.

Claim 10. (currently amended) The ~~method~~ system of claim [[1]]29 wherein the client identifying a requested form of access to the user-specific information in the data store and the access control engine ~~permitting~~ granting the requested access ~~client to have access~~ to the ~~requested~~ certain user-specific information in the data store if the user has granted said ~~the~~ form of access requested by the client ~~further~~ comprises[[:]] permitting the client to read the requested user-specific information in the data store and permitting the client to write the requested user-specific information in the data store.

Claim 11. (currently amended) The ~~method~~ system of claim 10 wherein permitting the client to read the requested user-specific information in the data store comprises accessing said ~~requested~~ certain user-specific information and transmitting a copy of the accessed ~~requested~~ certain user-specific information to the client in a SOAP message.

Claim 12. (currently amended) The ~~method~~ system of claim 10 wherein permitting the client to write the ~~requested~~ certain user-specific information in the data store comprises receiving at the web-services provider a SOAP message from the client identifying the ~~requested~~ certain user-specific information and writing the identified ~~requested~~ certain user-specific information in the data store.

Claim 13. (currently amended) The ~~method~~ system of claim [[1]]29 wherein ~~updating~~ creating the access control ~~list~~ rule to permit the client to have access to the ~~requested~~ certain user-specific information in the data store if the default access ~~control instruction~~ permissions permits the ~~determined~~ identified intended use ~~further~~ comprises[[:]] creating ~~updating~~ the access control ~~list~~ rule to permit the client to read the ~~requested~~ certain user-specific information in the data store[[;]] and creating ~~updating~~ the access control ~~list~~ rule to permit the client to write the ~~requested~~ certain user-specific information in the data store.

Claim 14. (canceled) ~~One or more computer-readable media having computer-executable instructions for performing the method recited in claim 1.~~

Claim 15. (currently amended) A method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider, ~~said web-services provider maintaining a data store of user-specific information associated with the user, said user-specific information accessible by the user and having access by the client controlled by the user, said client seeking access to certain of the user-specific information in the data store,~~ said method of controlling access to the user-specific information comprising:

operatively receiving at the web-services provider a request from the client to access the certain user-specific information in the data store wherein the web-services provider maintaining a data store of user-specific information associated with the user, said user-specific information accessible by the user and having access by the client controlled by the user, said client seeking access to certain of the user-specific information in the data store;

~~determining~~ generating an intended use request by the client of the certain user-specific information in the data store;

determining an allowed level of access permitted by the user;

comparing the ~~determined~~ generated intended use request with the determined allowed level of access;

invoking a consent engine in response to the client's request if the ~~determined~~ generated intended use request is outside the allowed level of access, said consent engine informing the user of the client's request to access the certain user-specific information in the data store and inviting the user to permit or to deny the client's request to access the certain user-specific information in the data store; and

completing the request from the client to access the certain user-specific information in the data store when the ~~determined~~ generated intended use request by said client of the certain user-specific information is within the determined allowed level of access permitted by the user.

Claim 16. (currently amended) The method of claim 15 wherein generating ~~determining~~ the intended use request by the client of the certain user-specific information in the data store comprises:

determining a type of information within the certain user-specific information in the data store that is being requested by the client; and

determining a form of access to the certain user-specific information in the data store that is being requested by the client.

Claim 17. (currently amended) The method of claim 16 wherein comparing the ~~determined~~ generated intended use request with the determined allowed level of access comprises:

determining if the user permits access to the type of information within the certain user-specific information in the data store that is being requested by the client; and

determining if the user permits the form of access to the certain user-specific information in the data store that is being requested by the client.

Claim 18. (currently amended) The method of claim 17 further comprising:

creating an access filter, said access filter defining an extent to which the user permits access to the type of information within the certain user-specific information in the data store and an extent to which the user permits the form of access to the user-specific information in the data store; and

wherein completing the request from the client to access the certain user-specific information in the data store when the ~~determined~~ generated intended use request is within the determined allowed level of access further comprises:

applying the access filter to the certain user-specific information in the data store to create a filtered information set; and

permitting the client to access the filtered information set.

Claim 19. (previously presented) The method of claim 15 further comprising denying the client access to the requested certain user-specific information in the data store if the determined intended use is outside the allowed level of access.

Claim 20. (canceled)

Claim 21. (original) One or more computer-readable media having computer-executable instructions for performing the method recited in claim 15.

Claim 22-28. (canceled)

Claim 29. (currently amended) A system for controlling access to user-specific information in a network computing environment, the system comprising:

a web-services service provider;

a user of a service of the web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user, said user-specific information accessible by the user and having access by the client controlled by the user, and a set of default access preferences defining a list of default access permissions allowed by the user;

a client of the web-services provider, said client generating a request~~ing~~ to access to certain of the user-specific information associated with the user ~~and~~ said request identifying an intended use by the client of the certain user-specific information in the data store;

an access control engine operatively receiving the client request to access the certain user-specific information and dynamically creating an access control rule by comparing the set of default access preferences with the intended use by the client, said access control rule granting the requested access by the client to the certain user-specific information if the intended use of the client of the certain user-specific information is within the list of default access permissions defined by the set of default access preferences allowed by the user; and

a consent engine generating an option list in response to the client's request for user-specific information having at least one entry therein based on the intended use by the client of the user-specific information in the data store, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

Claim 30. (original) The system of claim 29 further comprising a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device.

Claim 31. (canceled)

Claim 32. (currently amended) The system of claim [[31]]29 wherein the network communication device generates a selection signal indicative of whether the user accepted or rejected the at least one option displayed on the option menu.

Claim 33. (currently amended) The system of claim [[31]]29 wherein the consent engine provides a consent signal having a parameter indicative of whether the user accepted or rejected the at least one option and wherein the access control engine receives the consent signal, said access control engine granting the requested access if the consent signal indicates that the user accepted the at least one option.

Claim 34. (original) The system of claim 33 wherein the access control engine denies the requested access if the consent signal indicates that the user rejected the at least one option.

Claim 35. (original) The system of claim 29 further comprising an authentication engine authenticating a digital identity of the user and wherein the access control engine denies the requested access if the digital identity of the user is not authenticated by the authentication engine.

Claim 36. (original) The system of claim 29 further comprising a client intentions document identifying the intended use by the client of the user-specific information in the data store.

Claim 37. (original) The system of claim 36 further comprising:

a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device; and

a consent engine retrieving the client intentions document and generating an option list having at least one entry therein based on the intended use identified in the intentions document, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

Claim 38-46. (canceled)